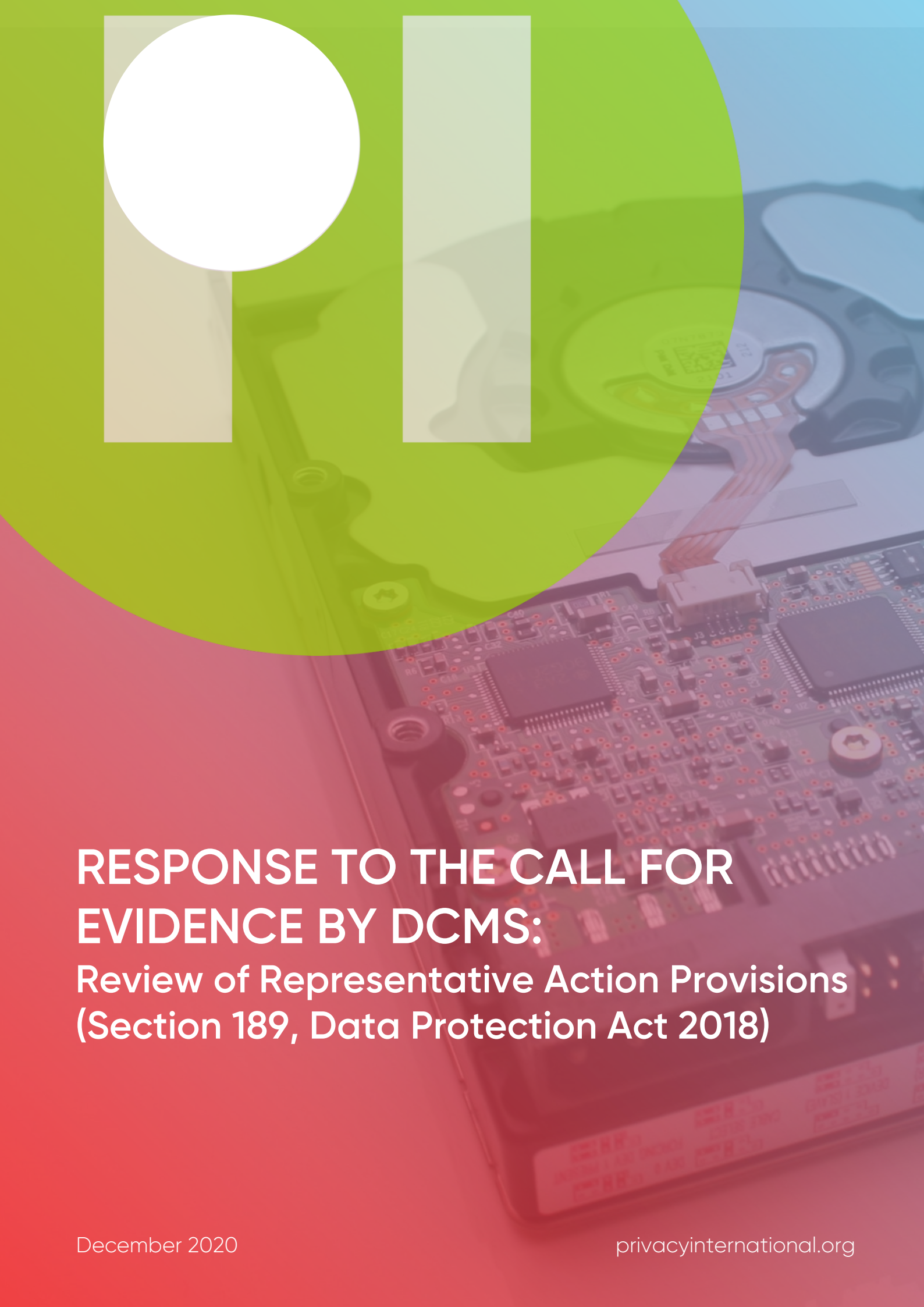


# RESPONSE TO THE CALL FOR EVIDENCE BY DCMS:

## Review of Representative Action Provisions (Section 189, Data Protection Act 2018)

December 2020

privacyinternational.org

# ABOUT PRIVACY INTERNATIONAL

Governments and corporations are using technology to exploit us. Their abuses of power threaten our freedoms and the very things that make us human. That's why Privacy International campaigns for the progress we all deserve. We're here to protect democracy, defend people's dignity, and demand accountability from the powerful institutions who breach public trust. After all, privacy is precious to every one of us, whether you're seeking asylum, fighting corruption, or searching for health advice.

So, join our global movement today and fight for what really matters: our freedom to be human.

**Open access. Some rights reserved.**

Privacy International wants to encourage the circulation of its work as widely as possible while retaining the copyright. Privacy International has an open access policy which enables anyone to access its content online without charge. Anyone can download, save, perform or distribute this work in any format, including translation, without written permission. This is subject to the terms of the Creative Commons Licence Deed: Attribution-Non-Commercial-No Derivative Works 2.0 UK: England & Wales. Its main conditions are:

- You are free to copy, distribute, display and perform the work;
- You must give the original author ('Privacy International') credit;
- You may not use this work for commercial purposes;

You are welcome to ask Privacy International for permission to use this work for purposes other than those covered by the licence.

Privacy International is grateful to Creative Commons for its work and its approach to copyright. For more information please go to www.creativecommons.org.

Privacy International
62 Britton Street, London EC1M 5UY, United Kingdom
Phone +44 (0)20 3422 4321
privacyinternational.org

Privacy International is a registered charity (1147471), and a company limited by guarantee registered in England and Wales (04354366).

Cover image: Vincent Botta

# RESPONSES TO CONSULTATION QUESTIONS

We welcome the opportunity to contribute Privacy International views and evidence in response to this important consultation. We are answering the questions that are relevant to our role, expertise and experience.

As we do not have competency and have not carried out research to address the particular needs of children, all the answers we give for the questions 12 to 20 below refer to all individuals.

1. **Are you responding to this consultation as:**

    a. A third sector organisation (registered Charity)

2. **What is your view on the uptake and operation of representative action provisions to date and what can be done to improve it? Please provide any relevant data and, where possible, make clear its source. For adults and children respectively, please explain what advice and support is currently available in relation to these provisions.**

    2.1 Privacy International (PI) does not have statistical evidence regarding uptake in the UK by non-profit organisations and operation of representative actions provisions in the Data Protection Act 2018, mandated by individuals. In the statistics provided by the ICO in the 2019 Annual Report, there's no breakdown on how many of the 38,514 complaints received were made by non-profit organisations on the authority of individuals, or the nature of such complaints; this seems to suggest that there were very few such complaints[1].

    2.2 Elsewhere in Europe there are more examples of non-governmental organisations having used representative actions under GDPR 80.1, principally by making complaints to the regulators following research and investigations, and then identifying individuals to represent. The best known is the Austrian organisation noyb - None of Your Business - (www.noyb.eu),

[1] Information Commissioner's Annual Report 2019-20, page 52 et ff https://ico.org.uk/media/about-theico/documents/2618021/annual-report-2019-20-v83-certified.pdf

and several examples are listed in its 2018-19 annual report[2]; of note is the complaint against social media apps on forced consent, on behalf of four users, which resulted in the biggest fine under GDPR to date: Euro 50 million to Google issued by the French authority, the CNIL. Noyb is also building up a comprehensive database of enforcement actions and cases throughout Europe, which includes the UK, and when fully populated will provide a useful resource[3]. With regards to taking cases to court representing one individual, organisations in Europe we have spoken to remark that such cases can take several years and finding individuals that are able and willing to stay the course is challenging.

2.3 Examples of complaints made by NGOs directly to the regulatory authority are more common throughout Europe. Whether authorities pursue these complaints or not is dependent on their resources and goodwill, since the majority are not mandated by law to pursue complaints by NGOs. Of note for the UK, Privacy International (PI) filed a formal complaint to the ICO (and two other authorities) to investigate potential GDPR infringements by data brokers, AdTech companies and credit referencing agencies. The ICO confirmed in January 2019 its focus on the AdTech industry, and published an update report in June 2019, citing PI's submission[4]. This report sets out that many of the industry practices are unlawful. The ICO paused further investigations due to the ongoing pandemic.

2.4 There are good reasons for what appears to be a very low uptake of representative actions authorized by data subjects, in our opinion. One is related to the fact that all the information gateways point to the data controller or regulatory authority as the right places to complain. Data controllers are required by law to give that information (GDPR Article 13.1 (b); a simple search online (e.g., 'data protection complaints' 'privacy complaints' 'where to complain' etc) will always come up with the ICO[5] or the government site which also points to the ICO[6].

2.5 Mention of the right to judicial remedy, or that individuals can instruct competent NGOs to complain on their behalf is rare or non-existent. Even a simple search of the Citizen Advice bureau website does not give such information. Apart from Which? who can offer advisory and legal services to

[2] https://noyb.eu/sites/default/files/2020-09/Annual%20Report_2018-2019.pdf
[3] https://gdprhub.eu/index.php?title=Welcome_to_GDPRhub
[4] https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf; PI's evidence is also cited in ICO's 2019 annual report
[5] https://ico.org.uk/make-a-complaint/
[6] https://www.gov.uk/data-protection/make-a-complaint

its members for a fee, we are not aware of other qualified not-for-profits, and that includes Privacy International, that offer such a service for individuals, which also explains the lack of information of on a service. Representing individuals in this manner is resource consumptive and may result in a resolution for one individual rather than correcting a systemic data protection problem which affects many. Therefore, we do not consider that it is the best use of resources for a privacy rights not-for-profit organisation.

2.6 Secondly, and we will cover this in more detail below, individuals tend to be alerted and complain about personal issues that have tangibly affected them or related to rights in the GDPR that have been widely popularised. Such issues include data breaches that can result in ID theft, credit reference and credit ratings issues or the right to access information, or nuisance calls. By far the biggest proportion of the 41,661 complaints in ICO's 201920 annual report concern subject access rights[7].

**3. What, if any, impact might these representative action provisions have had on people who identify with the protected characteristics under the Equality Act 2010 (i.e. age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation)? Please explain.**

3.1 We consider that the existing provisions for representative action brought on the authority of individuals are of little potential benefit to people with protected characteristics under the Equality Act 2010. This is due to the fact that by authorising a qualified organisation to take up a complaint on their behalf they would have to reveal sensitive private data – and few would be comfortable in doing this. For example, Privacy International's study of popular mental health websites (see Annex for a summary of this study) revealed widespread sharing of highly sensitive personal data with advertisers and data brokers. It is not likely that many people with mental health conditions would come forward individually about misuse of their information.

3.2 In another example, the Norway Consumer Council investigated the mobile app Grindr, which is a dating app for gay, bi, and trans (LGBT) people and found it to be sharing data such as Google Advertising ID, GPS location, gender, age, IP address and device information with 3rd party analytics and

[7] 46%, page 56

advertising companies, in breach of GDPR[8]. It is not likely that members of this community would come forward to complain about the misuse of their data either: the results of an EU survey by the Fundamental Rights Agency into the LGBT community show that they rarely report either discrimination or harassment to authorities, and many are not open about being LGBT with their family[9]. In these circumstances, organisations like Privacy International and the Norway Consumer Council would be better placed to bring a complaint based on the systemic problems they uncovered, allowing the concerns to be addressed without placing the onus on individuals to reveal sensitive private data.

**4. Do you think children's rights organisations should be permitted to bring claims on behalf of children in the same way as relevant non-profit organisations are able to currently? Please explain.**

4.1 Children's rights organisations are qualified and have the expertise to understand well children's development stages, and how they interact with online media; some, such as 5Rights, focus on children's digital rights and competencies and have a focus too on children's privacy. There are also not-for-profit organisations that represent other groups who identify with protected characteristics under the Equality Act 2010, and have a special understanding of the needs of these groups, and may have a focus on their human right to privacy.

4.2 Section 187 (4) of the Data Protection Act 2018 states that "The second condition is that the body or organisation is active in the field of protection of data subjects' rights and freedoms with regard to the protection of their personal data". This provision does not specify the nature of the organisation (e.g. consumer, or digital rights, or children's, etc.), or the segment of the UK population it should be focused on. Therefore, it seems that the law already allows such organisations to bring claims on behalf of children; equally an organisation that focuses on data protection of other communities, such as older people, and their data protection may also be permitted to bring claims on behalf of their particular constituency.

[8] https://www.forbrukerradet.no/side/new-study-the-advertising-industry-is-systematically-breaking-thelaw/
[9] https://www.scottishtrans.org/wp-content/uploads/2014/12/fra-eu-lgbt-survey-mainresults_tk3113640enc_1.pdf

4.3 The right to representation under GDPR 80.1 and Section 187 must not be limited, but apply broadly to non-for-profits that meet the conditions in Section 187 (3) and 187 (4) of the DPA 2018.

**12. Do you think the data protection legislation should be changed to allow non-profit organisations to act on behalf of individuals who have not given express authorisation? Please explain whether and why to permit such action in relation to the exercise of some or all of a data subject's rights.**

12.1 Privacy International firmly believes that the Data Protection Act 2018 should be revised to allow non-profit organisations to act on behalf of individuals who have not given express authorisation, as detailed in Article 80.2 GDPR. During the passage of the Data Protection Bill through Parliament, we have given detailed reasoning why this article must be implemented, as well as suggested amendments to ensure it is implemented[10]. These reasons remain fully valid, and key ones are summarized below (12.2 to 12.7). They are further strengthened by evidence collected in the intervening 17 months since implementation by Privacy International and others around Europe (see Annex).

12.2 There is a significant information and power asymmetry between individuals and those collecting and controlling their personal information. Some rights infringements of data protection are visible to individuals, and they constitute the bulk of complaints to the ICO (see answer to question 2 above). But there are many proven, hidden unlawful and potentially discriminatory practices that can affect hundreds of thousands of individuals, perpetrated by an unseen, large ecosystem of data mining entities, as well as by more public data controllers. Such practices can only be revealed by targeted investigations, often with the help of technologists or specialist software (see Annex for examples). The data mining business model is now considered so lucrative that many companies disregard the law; if the law was effectively enforced, those companies would be more ready to resort to other, still lucrative, but more privacy-protective business models.

[10] https://privacyinternational.org/news-analysis/1050/why-we-need-collective-redress-data-protection; https://privacyinternational.org/advocacy/2040/privacy-internationals-briefing-uk-data-protection-billhouse-lords-report-stage; https://privacyinternational.org/advocacy/677/privacy-internationals-briefingdata-protection-bill-second-reading-house-lords;

12.3 As many breaches of data protection law – such as unlawful data sharing or processing without a legal basis – affect hundreds of thousands of people rather than one individual, a mechanism for collective redress would save significant administrative and court time. Experience also shows that if cases are taken up for one individual only, infringing entities do not necessarily correct their practices to cover and benefit all individuals affected.

12.4 An 'opt-in' system of representation is not practical or efficient, whereby an organisation can represent a defined group of individuals, for a revealed data breach for example. It may be possible in a case where the impacted individuals are a clearly defined group and in a position to co-ordinate, such as the of Morrison's workers following a data breach[11]. It is not, however, practical in most situations, such as unlawful data sharing with third parties or across countries, and would not work where those affected may be a vulnerable group of individuals (so not able or willing to come forward).

12.5 In our briefing reports to Parliament during the passage of the UK Data Protection Act, we argued that failure to address vulnerabilities in internet-connected devices and apps threatens not only the safety of individuals, including children, but that such breaches of data protection have the ability to impact the UK economically, socially and politically[12]. Some of the people who invented these business models for the US technology giants are now denouncing them for their negative impacts and demanding appropriate legal remedies[13]. The GDPR is designed to address such issues, but to achieve improved controller practices there is need for effective enforcement. Implementing Article 80.2 GPDR can provide a powerful tool to achieve such enforcement.

12.6 The DCMS consultation paper mentions the risk of speculative, vexatious, 'ambulance chasing' claims which lack legitimacy and are a burden on resources. We are aware of such arguments, including on the part of some of the EU regulatory authorities. First, the current legislation has strict rules regarding the profile of organisations that can bring forward cases, including those which are authorised by an individual. For any

[11] https://www.theregister.com/2020/04/01/morrisons_wins_data_breach_vicarious_liability_supreme_court/

[12] https://privacyinternational.org/advocacy/2040/privacy-internationals-briefing-uk-data-protection-bill-house-lords-report-stage, page 13, para 4.4-4.5

[13] Documentary 'The Social Dilemma', available on Netflix; features interviews with former employees of Facebook, Google, and others.

qualified not-for-profit organisation, embarking on a collective action involves serious research, evidence building, legal expertise and a lot of resources. These are not actions to be undertaken lightly.

12.7 Arguments, as described in 12.6 above, disregard the evidence from other countries. There are all-encompassing collective redress systems in Belgium, France, Italy, Portugal, Spain, Sweden, Canada and Australia, and the Netherlands has recently introduced such a system[14]. Collective redress is not a new concept in the UK legal system either: such actions are already enabled under the Consumer Rights Act 2015 for any market failures that harm the interest of consumers. The Courts have safeguards in place to ensure that only cases of merit proceed, and such safeguards can be adapted to apply to a DPA collective redress regime.

12.8 After years of deliberation, the EU has recently passed the Collective Redress Directive, which will be implemented throughout the EU and the European Economic Area within the next two years. As outlined in the explanatory memorandum to the legislation[15], evaluations carried out in Europe demonstrated that risks of infringements of laws are increasing due to digitalisation and globalization, and enforcement of EU protection laws has not been effective. "*Consumers did not have all the right tools to seek justice – up to now. I am very pleased that these new rules will empower consumers to join forces and level the odds even in disputes with today's Goliaths*"[16].

12.9 The new Directive provides for designated qualified entities to seek injunctions and/or redress, including compensation, on behalf of a group of consumers. The scope of such collective actions include trader violations for a wide variety of consumer protection laws, including data protection. The rules strike a balance between access to justice and protecting businesses from abusive lawsuits, through measures similar to those in place for the UK 2015 Consumer Rights Act, such as courts' ability to dismiss unfounded cases; it also imposes on qualified not-for-profits a number of transparency requirements, for example with regards with their funding by third parties. Once this legislation is implemented, the UK will remain one of the very few countries in Europe without collective representative actions provisions,

[14] https://www.lexology.com/library/detail.aspx?g=a16c71b7-f453-4762-908a-c3e436f401f6
[15] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018PC0184
[16] EC Vice-President Vera Jourova
https://ec.europa.eu/commission/presscorner/detail/en/statement_20_1227

despite the government's stated commitment to maintain highest standards of consumer protection post Brexit[17].

**13. Should a children's rights organisation be permitted to exercise some or all of a data subject's rights on behalf of a child, with or without being authorised to do so? Please explain**

13.1 We assume this question refers to the exercise of data subject's rights under Articles 77, 78, 79 and 82 of GDPR, though Article 82, on the right to compensation, can only be exercised under Article 80.1, i.e. can only be authorised by an individual(s). Please see our answer to Question 4: there is nothing to preclude children's rights organisation to exercise these rights under the current provisions of GDPR and section 187 DPA 2018, which are widely expressed. Therefore we do not recommend that these provisions should be narrowed to particular types of organisations.

**14. What, if any, impact might allowing non-profit organisations to act on behalf of individuals who have not authorised them to do so have an impact on people who identify with the protected characteristics under the Equality Act 2010 (i.e. age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation)? Please explain.**

14.1 See our answer to Question 3. Allowing non-profit organisations to act on behalf of groups of individuals would be of benefit to people with the above-mentioned protected characteristics because they would not have to individually reveal personal highly sensitive data while action would be taken on their collective behalf to ensure lawful processing of their data. In the Grindr example (see box above and Question 3), the dating site for LGBT people, the Norway Consumer Council complained formally to its national regulatory authority[18]. If and when this infringement is investigated and action taken by the relevant authorities, all Grindr users will benefit. It is important to note that Article 80.2 of the GDPR does not give to non-profit organisations the right to claim compensation on behalf of the group of individuals represented. So even if – speculatively – judicial action was taken against Grindr on behalf of its users, the remedy would be an order to stop sharing sensitive user data with the identified third parties, to ensure lawful processing. No individual would need to come forward to get compensation, for example.

[17] https://www.gov.uk/government/news/government-affirms-commitment-to-strong-consumerprotections-post-brexit
[18] https://www.forbrukerradet.no/side/complaints-against-grindr-and-five-third-party-companies/

**15. What safeguards, if any, should operate to avoid the speculative or vexatious use of any new powers for non-profit organisations to act without the consent of individuals and avoid a disproportionate administrative burden on either the regulatory or courts systems?**

15.1 As outlined in 12.9 above there are existing laws that have safeguards in place to ensure the right balance between allowing access to justice and protecting entities from abusive lawsuits, such as allowing courts to dismiss cases that are considered without foundation. Collective redress laws that have such provisions also allow for compensation to be paid, which is not the case with Article 80.2 GDPR which only pursues a lawful data processing outcome.

15.2 This argument, regarding "vexatious" and "speculative" use of new powers by nonprofits, was also widely promoted by parliamentarians on the government side in the debates during the passage of the Data Protection Act 2018 – without bringing forward any factual evidence to support such claims. We are not aware of any evidence, for example, that any such powers are being used in an irresponsible way under the UK 2015 Consumer Rights Act. There is no evidence that EU Member States with functioning collective redress systems have an increase in litigation as a result. Even in the US, class actions do not constitute a significant part of all civil litigation cases (less than 1% of all civil suits)[19]. See also our answer in paragraph 12.6.

**16. What conditions, limitations or safeguards should apply if non-profit organisations act on behalf of individuals who have not authorised them to do so? For example, should individuals be given the right to object to a non-profit organisation taking action on their behalf without their consent? Please explain.**

16.1 As explained above, the legislation already provides for very strict rules of engagement for non-profit organisations even under Article 80.1 GDPR and Section 187 DPA 2018, and embarking on collective actions involves serious research, evidence building, legal expertise and a lot of resources. No organisations would undertake such an action lightly. Should further safeguards be necessary, the Courts have procedures and practices in place for the Consumer Rights Act, including only cases that

[19] https://www.law.berkeley.edu/wp-content/uploads/2019/10/Chapter-9-Deborah-Hensler.pdf, page 15

have merit can proceed, which could be adapted to apply to an Article 80.2 regime.

16.2 Regarding the possibility of giving individuals the right to object to a collective redress action that does not involve compensation, but is aimed at ensuring lawful processing of user data (as is the case with Article 80.2) which they have not authorised: first, the article as provided by GDPR does not require for any individuals to be named, so what would be the practical purpose or consequence of such objection? Would the action be stopped on the will of one individual? What if that individual has a conflict of interest, for example, is an employee or relative or friend of the defendant entity? There are a number of jurisdictions that allow for individuals to opt-out of collective redress actions, but we are not aware of any that provide for the right to object. A survey in 2011 by Eurobarometer on consumer attitudes towards consumer protection shows that in the UK 87 per cent of respondents would be more willing to defend their rights if they could join with other consumers that are complaining about the same thing[20]. It is not likely that attitudes have changed drastically since.

**17. If the new provisions discussed in this chapter were adopted, what impacts do you anticipate on data controllers which might be the subject of a complaint or legal claim, particularly businesses, including any increased costs or risks?**

17.1 This provision would be a good incentive for controllers, particularly businesses, to obey the law. Knowledge of poor enforcement encourages non-compliance, and conversely knowledge that public interest watchdogs have powers to take action encourages compliance with the law. The vast majority of complaints and legal actions brought forward by not-for-profit organisations throughout Europe under GDPR to-date have been directed at the big technology companies or AdTech, which profit from people's personal data, and have enough resources to put in place the right systems and procedures to comply with the legislation. As we mentioned above, the UK Information Commissioner refers to Privacy International's complaint on data brokers in its 2019 Annual report, and the preliminary conclusions of its investigation confirm PI's findings. Similarly, the French data authority has investigated Google and fined it

[20] Flash Eurobarometer 299, https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/FLASH /surveyKy/896/p/4 , page 56

Euro 50 million as a result of noyb's complaint. There are other examples around Europe of authorities taking up investigations as a result of research and complaints from not-for-profit organisations.

**18. If the new provisions discussed in this chapter were adopted, what are the likely impacts on the ICO or the judicial system, which will be required to consider representations made by non-profit organisations? What is their capacity to handle new claims brought under any new provisions, and how might the design of any new provisions help to manage pressures?**

18.1 Not-for-profit organisations throughout Europe have strongly argued for adequate resources to be given to the regulatory authorities in order to fulfil their enforcement duties effectively. Investigations and complaints by non-profits can alert the ICO to systemic infringements, as was the case with the Privacy International investigation and complaint regarding data brokers (see 12 above and Annex). One could also speculate that if more complaints were solved collectively, in time there would be fewer individual complaints, for example regarding data access rights which form a large proportion of the individual complaints to the ICO.

**19. What are the alternative means or mechanisms by which non-profit organisations are currently able to bring complaints to the ICO or to court using existing Civil Procedure Rules? Please provide any evidence of their use or operation to date.**

19.1 The existing mechanisms for collective redress in the UK are insufficient to guarantee that controllers and processors uphold and respect the rights of data subjects. Alternative means under existing Civil Procedure Rules are not easily accessible, if at all, for not-for-profit organisations, as they require complex administration and the kind of resources that only professional law firms have at their disposal. The most high-profile recent example is the case of Lloyd vs Google, allowed by the Court of Appeal to proceed as class action on an opt-out basis, with Mr Lloyd representing some four million affected individuals[21]. The case is now being appealed by Google in the Supreme Court.

19.2 More recently, we have the example the YouTube data breach claim, Duncan McCann vs Google, represented by a legal firm, and supported

[21] https://www.bailii.org/ew/cases/EWCA/Civ/2019/1599.html

with private finance backing; this is an opt-in representative action, and parents of children are invited to join[22].

19.3 Such examples are rare in the UK and show that under the current UK system the procedure is costly, complicated and not practical for use by most charities or not-for-profit organisations. It remains for now the domain of legal firms and private financing.

**20. In what ways would the potential measures outlined in Chapter 3 complement or duplicate these alternative mechanisms?**

20.1 There is no duplication. As we point out in many of our answers to this consultation, Article 80.2 GDPR is not a 'typical' collective redress mechanism, in that it does not provide for the right to receive compensation from the controller or processor for the damage suffered. It simply provides for the right to complain to an authority, and for the right to an effective judicial remedy. It provides for the practical possibility to enforce lawful processing requirements that affect a large number of people, and addresses practices that are not readily visible to individuals but that can be used as tools for discrimination, manipulation and exploitation, particularly of vulnerable groups. It is a step toward a more effective redress regime, to ensure that the DPA 2018 is practically enforced.

20.2 The attached Annex to the consultation includes recent research into practices that we believe are in breach of data protection legislation (GDPR and DPA 2018), and could be better addressed if the Article 80.2 redress mechanism is brought into force in the UK.

[22] https://www.youtubedataclaim.co.uk/

# Annex – the evidence

### Research by Privacy International and others

Investigations carried out by Privacy International and other digital rights and consumer organisations since the Data Protection Act 2018 was implemented show violations of GDPR that have not been effectively addressed to-date through enforcement actions. It is just a sample of existing evidence, and ongoing complaints that are carried out all round Europe targeting unlawful data protection practices of companies that operate internationally. These examples demonstrate a) that unlawful practices are carried out without individuals being aware, b) that they affect millions of people and c) that companies, even when urged directly to change practices or subjected to adverse publicity, still don't necessarily correct their unlawful practices.

### Challenge to Hidden Data Ecosystem:

On 8 November 2018, Privacy International filed complaints against seven data brokers (Acxiom, Oracle), ad-tech companies (Criteo, Quantcast, Tapad), and credit referencing agencies (Equifax, Experian) with data protection authorities in France (CNIL), Ireland, (DPC) and the UK (ICO). The complaints were based on over 50 Data Subject Access Requests (DSAR), as well as analysis of privacy policies and marketing promotions. This indicated wide-scale and systematic infringements of GDPR. Privacy International argued that these companies do not comply with the data protection principles of transparency, fairness, lawfulness, purpose limitation, data minimisation, and accuracy. Furthermore, they do not have a legal basis for the way they use people's data. The authorities were asked to further investigate these companies. In January 2019, the ICO confirmed its focus on the AdTech industry in the coming year, and in June 2019 published an update report into adtech and real time bidding, citing Privacy International's submission, which sets out that many of the sector's practices are unlawful. (The ICO investigation has been paused due to the pandemic situation). The Irish DPC and the French CNIL have also announced investigations following up on our complaint. For full details see https://privacyinternational.org/legal-action/challenge-hidden-data-ecosystem

### Investigation into tracking on mental health websites, including data sharing of depression tests:

A study by Privacy International published in September 2019 revealed how popular websites about depression in France, Germany and the UK share user data with advertisers, data brokers and large tech companies; some of these even leak answers and test results to third parties. The report highlighted how numerous mental health websites engage in programmatic advertising, a type of advertising that relies on sharing our personal data with hundreds if not thousands of companies to eventually serve us targeted ads. The findings raised serious concerns about compliance with European data protection and privacy laws. The goal of such research is not just to alert authorities and the public to unlawful company practices, but to push companies to change their behaviour. A second investigation into mental health websites in February 2020 revealed that a number of mental health websites did change their practices (including the NHS depression test site), but

others did not, including the French Doctissimo website, which was still sharing depression tests results directly with third parties. Consequently, on 26 June 2020, we filed a complaint against Doctissimo with the French data protection authority (CNIL). As a result of our complaint, the French authority launched an investigation in October 2020.

Follow these links for full details: https://privacyinternational.org/campaigns/your-mental-health-sale;
https://www.privacyinternational.org/news-analysis/3188/taking-depression-test-online-go-ahead-theyre-listening
https://www.privacyinternational.org/report/3351/mental-health-websites-dont-have-sell-your-data-most-still-do

Apps interactions with Facebook on Android devices:
Research by Privacy International in December 2018 revealed that Facebook (FB) routinely tracks users, non-users and logged-out users outside its platform through the Facebook Business Tools. At least 61 per cent of apps tested automatically transfer data to FB the moment a user opens the app. Some apps routinely send FB data that is very detailed and sometimes sensitive. A re-test in March 2019 found a number of apps corrected their behaviour, but many did not.

For full report and documentation see https://privacyinternational.org/appdata

Investigation into menstruation apps:
Millions of women share with menstruation apps their deeply intimate data - the date of their last periods, dates and details pertaining to their sex lives, their moods, their health. This data is being ruthlessly exploited and shared with third parties to target and profile people. Research (carried out December 2018) highlights that the menstruation apps Privacy International has exposed raise serious concerns when it comes to their compliance with their GDPR obligations, especially around consent and transparency. As a result of PI's research and advocacy on six popular menstruation apps, four of them made changes in their data sharing practices or launched internal investigations. Two of the apps have not made any changes.

For full information see https://privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruations-apps-are-sharing-your-data;
https://privacyinternational.org/taxonomy/term/676

Out of Control - investigation by Norway Consumer Council (NCC):
NCC is one of Europe's leading investigators of technology companies' privacy and data protection practices, with research that has looked into connected toys, deceitful online practices, and location tracking. Its latest report, published in January 2020, focuses on the analysis of data traffic from ten popular apps such as dating or period tracker apps, including the LGBT dating app Tindr. It exposes how a large number of mostly unknown third parties receive sensitive and personal data without the knowledge of the individual. Altogether, the ten analysed apps were found to transmit user data to at least 135 different third parties involved in

advertising or behavioural profiling. Such profiles can be used to personalise and target advertising, but also end up being tools for discrimination, manipulation and exploitation. Some dating apps were found to be sharing sensitive data about sexuality, drug use and political views. More than 100 consumer, digital and civil rights organisations round the world, including in the UK, partnered for joint action and complaints to authorities as a result of this research.

For all the details and full report see:
https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/report-out-of- control/ ; https://www.forbrukerradet.no/side/complaints-against-grindr-and-five-third- party-companies/

**Privacy in the EU and the US - consumer experiences across three global platforms:**
research by the Transatlantic Consumer Dialogue (TACD) into data protection practices by three global platforms – Amazon, Netflix and Spotify – set out to find out whether users in the US are treated differently in terms of data protection practices than users in the EU, but in fact revealed possible infringements of GDPR by these big global companies in the EU as well. The research used 'mystery shopping' techniques (including in the UK) and detailed analysis of privacy policies, and its findings revealed unavoidable tracking, including by third parties by default, policies too complicated to read and understand by most people, and use of the so-called "dark patterns", i.e. user manipulation by design, nudged into least privacy-friendly choices.

Full report: http://tacd.org/tacd-and-heinrich-boll-stiftung-brussels-publish-research-highlighting-failings-in-privacy-protection-on-both-sides-of-the-atlantic/

**Timeline of complaints against AdTech companies**
The General Data Protection Regulation (GDPR) became enforceable on May 25th 2018. Since then, complaints against the AdTech industry are piling up, attacking intrusive tracking and profiling practices, unfairly obtained consent and insufficient legal basis, all of which we consider to infringe GDPR. The timeline below gives a list of some of the key actions taken against this ecosystem, a demonstration that GDPR still has to be implemented and enforced.
https://privacyinternational.org/adtech-complaints-timeline

**September 2018:** Regulatory complaint against Google and other "ad tech" companies under Europe's GDPR by Johnny Ryan, Jim Killock, and Michael Veale

**November 2018:** Privacy International files complaints against seven companies for wide- scale and systematic infringements of data protection law

**January 2019:** Panoptykon Foundation files complaint against Google and other "ad tech" companies with the with the Polish Data Protection Authority

**April 2019:** Formal GDPR complaint against IAB Europe's "cookie wall" and GDPR consent guidance, by Dr Johnny Ryan
**May 2019:** Data Protection Commission opens statutory inquiry into Quantcast International Limited following Privacy International submission

**May 2019:** Ad Tech GDPR complaint is extended to four more European regulators

**January 2020:** Complaints against Grindr and five ad tech companies are filed at the Norwegian Data Protection Authority by the Norwegian Consumer Council (Forbrukerrådet) and noyb (https://noyb.eu/en)

**June 2020:** Privacy International files a complaint against Doctissimo before French Data Protection regulator

**October 2020:** Formal complaint against Vienna-based address broker is laid before the Austrian Data Protection Authority, by noyb.

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org

Privacy International is a registered charity (1147471), and a company limited by guarantee registered in England and Wales (04354366).